ANNUAL DISCLOSURE & INFORMATION SECURITY TRAINING BOOKLET

State of California

Franchise Tax Board

Privacy, Security, and Disclosure Bureau

All FTB Employees

The issue of information privacy and security has been propelled to the forefront of public interest due to the rise in identity theft and the theft or loss of confidential information. Each time a taxpayer sends us their confidential personal and financial information, they are entrusting us to keep their personal tax information private. Our job of safeguarding confidential information is essential to continued taxpayer confidence and support.

To address the public's privacy concerns, we created the Information Privacy Principles for Individuals based on the California Information Practices Act. These eight principles can be found on the FTBNet2, and defines our ongoing commitment to protect confidential taxpayer information while using it responsibly. Your program area is entrusted to meet the standards set forth in these principles, and your management may be asked to certify that their program is in substantial compliance with these principles.

Each year, it is mandatory that you complete Disclosure Training. This is part of our commitment to the Information Privacy Principles for Individuals, as well as federal and state requirements. Under these laws, you may only access information you have been authorized to see and have an appropriate business need to use. These laws also state that you may not disclose or share any personal information with others without proper authorization. By completing this training, you are not only acknowledging your understanding of these concepts, but you declare your personal commitment to maintaining the confidentiality and privacy of taxpayer information.

The Franchise Tax Board is a highly respected tax agency that places a tremendous amount of importance on ensuring the confidentiality, integrity, and availability of FTB's information systems and the information they contain. I am confident you will continue to build on our reputation by serving the public to the best of your ability and by continually protecting the privacy and security of information at FTB.

Selvi Stanislaus

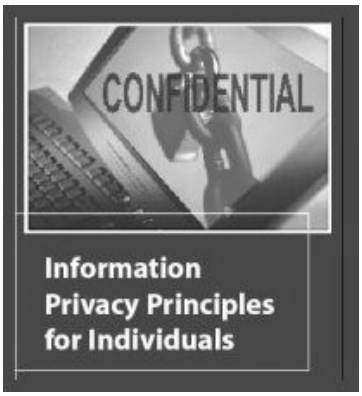
Executive Officer

Table of Contents

Table of Contents

INFORMATION PRIVACY PRINCIPLES FOR INDIVIDUALS

Introduction to Information Privacy Principles for Individuals



The growth in identity theft has increased the public's concerns about information privacy and security. Our job of safeguarding confidential taxpayer information has never been more important or challenging. To address the public's concerns regarding their privacy, the Information Privacy Principles for Individuals (IPPI) were created. These principles are based on the California Information Practices Act.

The California Information Practices Act (IPA) provides individuals the right to access personal information about themselves in State records. The IPA provides that agencies are obligated to allow individuals to inspect their "personal information" with exceptions, in certain "records containing personal information" (Civil Code Section 1798.34).

You are required to complete the Annual Disclosure & Information Security Training each year. Completing the training fulfills the federal and state law requirements placed on us and meets the standards defined in the IPPI.

To help you become familiar with the IPPI, we have provided a single-paged reference (refer to page 7) to tear out and use as a reminder.

By becoming familiar with the IPPI,
you will be able to identify how they apply to your job
and put them to work!

This page left intentionally blank.

tear out

INFORMATION PRIVACY PRINCIPLES FOR INDIVIDUALS

1. Information Gathering and Use Principle

We gather personal information only if it is relevant and necessary for us to accomplish our mission. We use personal information in a responsible and lawful manner.

- We gather personal information only after we determine we have an appropriate use for it.
- We strive to use only information that is accurate, complete, and current.
- If we use personal information for other than the original intended purpose, we first determine that the new use is appropriate.

2. Information Sharing Principle

We share personal information only when we have legal authority to do so.

- We do not share personal information with others unless: (a) you have given us the authority to share the information, or (b) the other party has legal authority to receive the information.
- We educate others with whom we share personal information on the requirement to protect privacy.

3. Information Retention Principle

We retain personal information only as long as necessary to fulfill established business needs for that information.

- We periodically review our business needs to retain personal information.
- We destroy the personal information we no longer need.

4. Information Security Principle

We have reasonable safeguards to ensure the security and confidentiality of personal information.

- We educate our employees on the importance of protecting the privacy of personal information.
- We protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification.
- We provide personal information only to employees who have a business need and only when appropriate safeguards are in place.
- We tailor our safeguards based on the type of information we maintain.
- We periodically review our practices to ensure we have adequate safeguards.

5. Right to Know Principle

Individuals have the right to know what types of personal information we gather and use.

- We will tell you what types of personal information we gather and how we use the information.
- We will tell you what types of personal information we share with other organizations and the authority for sharing the information.
- We routinely inform the public about our information privacy policies and practices.
- We provide, upon request, information about our privacy policies and practices, including the names of staff responsible for overseeing our compliance.

6. Right to Inspect & Correct Principle

Individuals have the right to inspect the personal information we maintain about them and to request that we correct errors.

- We have an accessible and simple inspection and correction process.
- We respond to your request within a reasonable time and at minimal or no cost to the individual.
- We correct the personal information when more accurate or compete facts are established.

7. Right to be Heard Principle

You have a right to be heard if you believe we failed to adhere to our Information Privacy Principles for Individuals.

- We have an accessible and simple complaint process.
- We investigate all complaints and respond promptly.
- We take corrective measures when appropriate.

8. Commitment Principle

We periodically have outside privacy experts review our practices to ensure that we follow our Information Privacy Principles for Individuals.

This page left intentionally blank.

Introduction to Information Protection

Franchise Tax Board (FTB) receives and maintains tax and non-tax information. Some of this information is public and some is confidential.

This booklet will help you to understand the difference between confidential and public information and to determine when it's okay to access, acquire or disclose confidential information.

We have provided a glossary of key terms located at the back of this booklet. You will need to become familiar with the key terms to assist in your understanding of disclosure practices.

Confidentiality and Right of Access

All tax returns, return information, personal data, and proprietary information should be considered confidential unless it is specifically defined as public information through statute, rule, or regulation.

San Diego Field Office

Houston Field Office

The right of access is contingent on the individual having the statutory authority to obtain the information, such as when a third party holds a power of attorney.

California Law [1]

California law provides for the confidentiality of tax data, right of access, and penalties for any misuse of confidential information.

Under California Law, it is a misdemeanor for you to inspect, disclose or use confidential information without a business need to do so.

The fine is up to $1,000, up to six months in jail, or both.

If the unauthorized disclosure involves the use of a state computer, the disclosure may be prosecuted as a felony.

State Capitol

New California Law

Effective January 1, 2007, SB 25 (Civil Code 1798.85(a)(5)) prohibits state agencies from sending the Social Security Numbers (SSNs) **by mail** to the taxpayer, except in certain specific situations where required by law.

Exceptions to SB 25:

- Mailings to any third party (financial institutions, employers, other public agencies) may contain the SSN.
- Mailing to taxpayer representatives may contain the SSN, but use caution if a copy is sent to the taxpayer, as the SSN must be redacted.
- Mailings where other state or federal law requires the SSN. Examples include IRS documents (RAR, CP2000, and 1099s).
- SB 25 does not prohibit taxpayers from putting the SSN on tax returns. Taxpayers will continue to use the SSN on their returns.
- SB 25 does not prohibit FTB from using the SSN for internal systems.

Please contact your supervisor for how this impacts your business area.

[1] California Revenue and Taxation Code Sections 19542 through 19568

Federal Law [2]

Federal law provides that states administering income tax can have access to IRS data.

It also provides for penalties for unauthorized disclosure and unwarranted browsing (also known as UNAX).

Under federal law, it is a felony to make an unauthorized disclosure of federal tax information (FTI). The penalty shall not exceed $5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution.

In addition, browsing of FTI is punishable by a fine not to exceed $1,000, or imprisonment of not more than 1 year, or both, together with the costs of prosecution.

Under federal law, the taxpayer can file a private lawsuit against you, either for browsing or unauthorized disclosure.

[2] Internal Revenue Code Sections 6103(d), 7213, 7213(a)(2), and 7431

PILLARS OF INFORMATION PROTECTION

As an FTB employee you have a responsibility to protect the confidential information maintained by the department.

You provide the foundation for the department's information protection. In fact, the department's information protection "system" can be thought of as three Pillars of Information Protection: Access, Disclosure, and Acquisition.

Pillar I – Access

Accessing confidential information must be limited to your need to know to perform your official job responsibilities.

Pillar II – Disclosure

It is the responsibility of FTB employees or agents to ensure that confidential information is not disclosed to unauthorized persons.

Pillar III – Acquisition

Acquisition is printing, writing, or committing to memory specific personal information as defined by California Civil Code section 1798.29.

Accessing confidential information must be limited to your need to know to perform your official job responsibilities.

The topics covered in the first Pillar include:

- **Information Security**
- **Unauthorized Access (UNAX)**

Information Security

Everyone's Responsibility

Information Security is everyone's responsibility. Users of FTB information, whether employed by FTB, another department, or contract personnel must:

1. Use FTB information assets only for authorized purposes in accordance with their job duties.

2. Comply with applicable laws, administrative policies, and security policies and guidelines.

Things You Should Know

- Workstation Security
- Protecting Information from Loss or Theft
- Unauthorized Software and Hardware Devices
- Internet Usage
- Email and Instant Messaging Usage
- Security Incidents – What to Do
- Teleworking Guidelines

Workstation Security

You are responsible for ANY activity that takes place under your User ID. Taking appropriate measures will help safeguard not only yourself, but also taxpayer information.

Prevent unauthorized activity by:

- Never letting anyone use your User ID or password/pass phrase to logon.
- Always locking or shutting down your computer when unattended.
- Never share your password with anyone, not even your supervisor or Helpdesk staff.

Protecting Information from Loss or Theft

- Keep a "clean desk" – never leave confidential information visible and unattended. Cover or turn over confidential documents.
- If you must travel with confidential information, keep it covered with form FTB 7805 – *Confidential Cover Sheet*.
- Do not leave your desk or FTB facilities with confidential information unless you have a business need and permission to do so.
- Confidential information on portable computing devices and electronic media such as laptops, personal digital assistants (PDAs), CDs, flash drives, and diskettes must be encrypted.
- Use appropriate confidential destruct boxes/bins.
  - ✓ **Recycle Bin** (Non-Confidential Documents ONLY) – Confidential information or trash should never be placed in these bins. When in doubt whether a document is confidential, use a confidential destruct container.
  - ✓ **Confidential Destruct Box** – Confidential documents and records must always be placed in the proper container. All confidential destruct boxes must have form FTB 7055, *Destruction-Certified-Confidential Material* (the light blue form) attached to at least two sides of the box.

Unauthorized Software and Hardware Devices

The PC Helpdesk has current procedures and processes that keep all department PCs standardized, licensed and secure. If you need assistance with your FTB computer, call the PC Helpdesk.

- Do not install software on or remove software from an FTB PC unless you have written authorization.
- Do not install or connect hardware devices such as modems, flash dries, personal digital assistants (PDAs), advanced cellular phones, cameras, etc., on an FTB PC unless you have written authorization.
- Personal portable media such as diskettes and CDs can contain viruses. Do not bring portable media in from an outside source and insert into an FTB PC.

Internet Usage

The Internet is provided as a tool to support various business functions throughout the department. All websites accessed must be appropriate for the work environment.

DO NOT download software or unauthorized files from the Internet. FTB must adhere to licensing and copyright laws.

For FTB's acceptable Internet use policy, refer to the Information Security Policy (ISP) file, located on the FTBNet2.

If you are still uncertain of acceptable usage of the Internet, talk to your supervisor.

Email and Instant Messaging Usage

Email and Internal instant messaging are essential business tools, however, they are unsecured methods of communication. If you must email confidential information to FTB employees within the FTB email system, label the message “Confidential” or “Sensitive”.

For guidelines on the acceptable use of email and instant messaging, see the PC Helpdesk web page on the FTBNet2.

To keep confidential information secure, **DO NOT**…

- Send emails (including internal emails) with confidential information listed in the subject field (Social Security Numbers, taxpayer names, etc.)
- Send emails containing confidential information **outside** the department. This includes other state agencies such as the Board of Equalization (BOE) and the Employment Development Department (EDD).
- Send or forward chain mail – you can’t control what comes into your email inbox, but you can control what goes out.
- Use your FTB email address to register for non-business related events. This encourages SPAM (unsolicited email).

Security Incidents – What to Do

- Receive a suspicious email?
- Computer not working correctly?
- Do you think you may have a computer virus?

Report these security incidents right away by calling the PC Helpdesk at ((****)). Immediate response can help contain the problem and keep it from growing.

Immediately report the loss or theft of computer equipment or the theft of FTB information to FTB Security at ((****)).

NOTE: ((****)) = Indicates confidential and/or proprietary information.

Teleworking Guidelines

Having the same data and application privileges when working away from the office enhances our work productivity at home or on the road. However, teleworking introduces additional security concerns.

When working away from the office, your work behavior can help reduce security risks considerably. Use the teleworking guidelines when working away from the office.

- At all times, FTB employees must only use FTB owned equipment to connect to the department's internal network.
    - If accessing ((****)) ONLY from an offsite location, it is not required to use FTB owned equipment.
- Keep the computer's operating system and applications updated with the most current patch levels.
- Do not use unauthorized software or hardware.
- Keep virus definitions updated.
- Be aware of your surroundings and others around you when looking at confidential information.
- Consider working in a private room.
- When your computer is unattended, lock your PC and shut the door of the room you are working in.
- When on the road, keep your laptop with you or locked in the trunk of your car.

Report any inappropriate activity to the Privacy, Security, and Disclosure Bureau at((****)).

NOTE: ((****)) = Indicates confidential and/or proprietary information.

Unauthorized Access (UNAX)

Taxpayer Browsing Protection Act of 1997 briefly states: Willful unauthorized inspection or access of federal tax information (also known as browsing) is illegal. The word UNAX was created from the Federal Law [3]. UNAX stands for *"unauthorized access".* Browsing is in violation of federal and state laws written to protect individuals' right to privacy.

You should never access any confidential information, either in electronic or paper format, without an official business-related need to know. NEVER access, attempt to access, or modify accounts pertaining to you, family members, friends, acquaintances, co-workers, etc.

Examples of UNAX:

- Curiosity (for example, looking up celebrities).
- Personal use (for example, looking up an address).
- Nosiness (for example, "How can my neighbor afford a swimming pool?").
- Personal or monetary gain (for example, need to know someone's income for child support).
- Intentional harm (i.e., accessing addresses for retaliation).
- Prior work assignments (i.e. looking up a case no longer assigned to you).

If an employee willfully browses (makes a conscious decision to inspect information without proper authorization) confidential information, the punishment may include:

- Up to a $1,000 fine and/or imprisonment of up to one year, by the *federal government*; and/or
- Up to a $1,000 fine and/or up to six months in the county jail, by *state government*; and/or
- Disciplinary action, including termination by the *Franchise Tax Board.*

If you make an accidental or inadvertent access to an account (yourself, friend, neighbor, etc.) you must report the access to your supervisor. Your supervisor will notify Security Audit and let them know an inadvertent access was made.

[3] California later conformed to this federal law with its own code, R&TC 19542.1.

Unauthorized Access (UNAX)

Never access, attempt to access, or modify accounts pertaining to you, family members, friends, acquaintances, co-workers, etc.

Looking up information just for your personal use or curiosity or even attempting to do so can result in ANY of the following disciplinary actions:

- Criminal prosecution
- Loss of employment
- Demotion
- Suspension

When an employee leaves FTB, all access privileges must be immediately revoked or suspended.

Disclosure restrictions and the penalties apply even after employment with Franchise Tax Board has ended.

Changes to the FTB employee's system and facility access (physical and logical) are the responsibility of the employee's supervisor or manager at the time of the separation or transfer.

Browsing confidential information on another employee's desktop, computer, in-basket, or confidential destruct box is a CRIME!

PILLAR II – DISCLOSURE

It is the responsibility of FTB employees or agents to ensure that confidential information is not disclosed to unauthorized persons. The topics that will be covered in the second Pillar include:

- **Internal Revenue Service**
- **Authorized Disclosures**
- **Unauthorized Disclosures (UAD)**
- **Reporting**

Internal Revenue Service

FTB receives confidential data from the IRS referred to as *Federal Tax Information (FTI)*.

All information received from the IRS is subject to federal law. Federal law makes it a *felony* to disclose FTI except as necessary for tax administration purposes.

Our exchange agreement using IRS data has restrictions and guidelines including:

- Flagging – Form FTB 7805, *Confidential Cover Sheet,* is used for labeling or the marking of FTB files and storage area identifying FTI.
- Locking up FTI during non-office hours.
- Not sending FTI to any other agency without written permission from the IRS.
- Accounting for receipt, use and destruction of FTI.

Important Reminder: When FTI is commingled with FTB files, either paper or electronic, it is still considered IRS information and is subject to federal requirements of nondisclosure and confidentiality safeguards.

Authorized Disclosures

Ask this question before you disclose information:

Is the information public or confidential?

- If the information is **public**, anyone and everyone has the right to see or use the information. You may disclose the information.

- If the information is **confidential,** does the individual have the right to obtain the information?

Generally, confidential taxpayer information (except IRS information) may be disclosed to the following:

- Taxpayer
- The taxpayer's authorized representative
- Multistate Tax Commission
- FTB employee having the need to know
- Authorized designees with whom we have an exchange agreement as shown below:
    - IRS
    - California Secretary of State
    - Employment Development Department
    - State Board of Equalization
    - State Controller's Office
    - Other State's tax departments

The Disclosure Section maintains records of the Franchise Tax Board employees, IRS, and other agency's employees authorized to request, receive, and release confidential tax information.

Designee Lists are maintained on the Disclosure Section homepage..

If you are unsure whether or not a person is an authorized designee, contact the Disclosure Section ((****)).

NOTE: ((****)) = Indicates confidential and/or proprietary information.

Unauthorized Disclosures (UAD)

Unauthorized Disclosures are commonly known as UADs. An Unauthorized Disclosure is making confidential information known to an individual or entity that is not authorized to obtain, view, or use the information in any manner.

Most UADs are unintentional or accidental; however, some UADs are intentional. You will become familiar with both scenarios and the steps to take if they occur.

As an FTB employee, you must honor the public's constitutional right of privacy and respect other people's desires to keep their personal information secure from unauthorized disclosures.

Intentional UAD

Intentional UAD is knowingly giving confidential information to an individual, entity, or agency that is not authorized to obtain, view, or use the information in any manner.

Intentional disclosures may be punishable under State and Federal law.

Disclosure restrictions and the penalties apply even after employment with the Franchise Tax Board has ended.

Unintentional Disclosure

An unintentional UAD of confidential information may include the following examples:

- Phone conversation regarding account information with the wrong taxpayer.
- Mailing machine stuffing malfunctions (e.g., two or more different taxpayers' bills or notices sent in the same envelope).
- Misdirected faxes of confidential information.
- Disclosure without a valid Power of Attorney and/or proper authorization.
- Loss or theft of state property (computer or briefcase) containing confidential information.
- Mail sent to the taxpayer's address of record but opened by a third party. (While this is technically not an unauthorized disclosure, it should be reported to the Disclosure Section.)

Reporting

The Disclosure Access Reporting and Tracking System (DARTS) is an automated system for FTB supervisors and employees to report all UADs to the Disclosure Officer. It provides a consistent method of capturing necessary information about an incident, including the employee involved, the taxpayer, and incident details.

Take the following steps to complete the report of a UAD.

Step 1: Report all UADs to your supervisor immediately. (This includes those observed and overheard, as well as disclosure due to your own actions.)

Step 2: The supervisor completes the report using DARTS on FTBNet2.

Step 3: When the DARTS web-form is complete, an email will be sent to the Disclosure Section.

Remember: It is critical that ALL unauthorized disclosures be reported to your supervisor and in DARTS immediately.

PILLAR III – ACQUISITION

Acquisition means printing, writing, or committing to memory specific personal information as defined by California Civil Code section 1798.29. The topic covered in Pillar III is:

- **Unauthorized Acquisition (UAA)**

Unauthorized Acquisition (UAA)

Unauthorized Acquisition (UAA) means to take specific computerized personal information that compromises the security, confidentiality, or integrity of that personal information. FTB is required to notify the taxpayer when this occurs.

This law became effective on July 1, 2003, with the passage of AB700, California Civil Code section 1798.29.

Personal Information Defined

Personal information, as defined in the law (California Civil Code section 1798.29) is a person's first and last name in combination with one or more of the following:

- SSN
- California Driver's License Number
- Identification Card Number
- Bank Account Number, Credit or Debit Card Number along with the security, access, or password code that would permit access to financial records.

FTB is required to notify the taxpayer of the occurrence in accordance with California Civil Code section 1798.29.

If the taxpayer requests the name of the employee who inappropriately obtained their information, FTB will generally provide the taxpayer with the name of the employee.

Penalties

Taxpayers can sue the employee who acquired their information for up to $2,500 per occurrence, including any additional amounts for damages.

You will be personally liable for any monetary awards determined by the court and the taxpayer will know you acquired their information.

Don't take ANY information…IT'S A CRIME!

KEY TERMS

Becoming familiar with the *Key Terms* will assist in your understanding of disclosure practices.

.....

Access – The ability or privilege to make use of confidential information as an employee or agent of FTB.

Acquisition – Committing to memory, printing or writing down confidential personal information as defined by California Civil Code section 1798.29.

Authorized Representative – Individuals to whom taxpayers have given authority to act on their behalf through a power of attorney, as well as anyone they have given authority to view their confidential data via waivers, releases, or declarations.

Confidential Information – Confidential information is any information that is submitted to, or developed within the Department to administer its programs and is not specifically made public by statute.

The following types of information are considered to be "confidential" and should not be disclosed to unauthorized persons.

1. *Personal Income Tax*

    - Social Security Number
    - Taxpayer Return Information
    - Taxpayer Name/Address

2. *Corporate Income Tax*

    - Financial Information and Other documents filed with FTB

3. *Other*

    - Proprietary Information
    - Information Related to Any Current or Potential Audit/Investigation Activity
    - Official Personnel File Information

Disclosure – Making information known in any manner, such as by phone, fax, letters, or discussion.

Need to Know – Accessing confidential information must be limited to what you have the need to know to perform your official job responsibilities as an employee of the Franchise Tax Board.

Without the need to know you are not authorized to access, attempt to access, request, or modify confidential information.

KEY TERMS

Proprietary Information [4] – Information that is owned or developed by a company or government agency and should not be disclosed to unauthorized persons. Proprietary information is always considered confidential. For example:

- Navigation keys for FTB systems.
- Transaction procedures for FTB systems.
- Information that seriously impairs the assessment, enforcement, or collection of tax.
- Selection criteria.
- Hardware and software configuration information (program numbers, data flow diagrams, Internal Networking Paths).

Public Information – Public information is information that anyone and everyone has the right to see or use. Public information is determined by statute, rules, regulations, and policy. Some examples are:

1. *Corporate Income Tax*

    - Corporation Name
    - Corporation Address
    - Date Corporation Return Filed
    - Corporation Identification Number

2. *Other*

    - Specific Portions of FTB Employees' Personnel Records
    - Employee Newsletter
    - Public version of the Collection Program Manual

Redaction – The editing of a document to remove confidential and proprietary information.

Unauthorized Disclosure (UAD) – An Unauthorized Disclosure (UAD) is making confidential information known to an individual or entity who is not authorized to obtain, view, or use the information in any manner.

[4] R&TC Section 19544 and specific portions of the Government Code exempt proprietary information from disclosure.

INSTRUCTIONS FOR CERTIFICATE AND CONFIDENTIALITY STATEMENT

The following pages of this Annual Disclosure & Information Security Training Booklet contain the Disclosure Education Quiz, the Certificate of Completion and the Confidentiality Statement. Each of these forms **must be completed** and given to your supervisor.

After completing the mandatory Disclosure Education Quiz located on page 23, please do the following:

1. Certificate of Completion – Fill out the bottom portion of the Certification of Completion (located on the reverse side of the quiz), tear it out and give it to your supervisor.

2. Confidentiality Statement – Read each section of the Confidentiality Statement and initial. Sign and date the bottom portion of the statement, tear it out and give it to your supervisor.

This page left intentionally blank.

tear out

DISCLOSURE EDUCATION QUIZ

Please circle the correct answer. On multiple-choice questions, more than one answer may be correct. The answers to these questions can be found on the bottom of page 27.

1. *True or False* – All tax returns, return information, personal data and proprietary information should be considered and treated as confidential information.

2. *True or False* – If an unauthorized disclosure involves a state computer, the disclosure may be prosecuted as a felony.

3. *True or False* – Under federal law, the taxpayer can file a private lawsuit against you for browsing or disclosing confidential information.

4. *True or False* – It's okay to leave your computer unlocked while on break.

5. *True or False* – You may load personally owned software on your computer, as long as you are careful.

6. *True or False* – UNAX refers to the unauthorized browsing or accessing of confidential information, whether on paper or in electronic format.

7. *True or False* – You move to a new unit and your old workload is reassigned. It is okay to access an account from your old workload without a business need.

8. *True or False* – You may access your own account on the Taxpayer Information (TI) system.

9. *True or False* – When commingled with FTB files, IRS information is not subject to federal law.

10. *True or False* – You must flag all IRS information.

11. *True or False* – FTB can share IRS information with other agencies without written permission from the IRS.

12. *True or False* – Taxpayers will be notified when it is discovered that their data was acquired by an unauthorized person.

This page left intentionally blank.

State of California

Franchise Tax Board

Privacy, Security, and Disclosure Bureau

Certificate of Completion

This certifies that _____ has completed the

(Employee name)

Annual Disclosure & Information Security Training

on this date _____.

(Date completed)

Authorized by_____

(Supervisor signature)

Employee user id: _____

Employee payroll unit code: _____

This page left intentionally blank.

tear out

STATE OF CALIFORNIA
FRANCHISE TAX BOARD

CONFIDENTIALITY STATEMENT

I, _____ an employee of _____
PRINT YOUR NAME PRINT YOUR EMPLOYER'S NAME

hereby acknowledge that confidential information is protected from disclosure by law, regulation, and policy. I further acknowledge that protecting confidential information is in the public's interest, the state's interest, and my own personal interest. I also acknowledge that the Franchise Tax Board strictly enforces information security.

State employees and contractors:

I, _____ INITIALS agree to protect the following types of confidential information:
- Tax account information;
- Taxpayer and feepayer information;
- Claimant and employer information;
- Information about individuals that relates to their personal life or identifies or describes an individual;
- Internal Revenue Service's confidential and proprietary information;
- Other agencies' confidential and proprietary information;
- Criteria used for initiating audit selection;
- Methods agencies use to safeguard their information, including computer systems, networks, server configurations, etc; and
- Any other information that is considered proprietary, a copyright, or otherwise protected by law or contract.

I, _____ INITIALS agree to protect confidential information by:
- Accessing, inspecting, using, disclosing or modifying information *only* for the purpose of performing official duties;
- Never accessing, inspecting, using, disclosing, or modifying information for curiosity, personal gain, or any non-business related reason;
- Never attempting to access, use, disclose or modify information for any non-business or personal reason;
- Securing confidential information in approved locations; and
- Never removing confidential information from my work site without authorization.

I, _____ INITIALS acknowledge that as a State employee or contractor, I am required to know whether information I have been granted access to is confidential. If I have any questions, I will contact my agency's Disclosure Officer or Information Security Officer.

I, _____ INITIALS acknowledge that unauthorized access, inspection, use, or disclosure of confidential information is a crime under state and federal laws, including but not limited to: California Revenue and Taxation Code sections 19542, 19542.1, and 19552; California Penal Code section 502; California Unemployment Insurance Code sections 1094, 2111, and 2714; California Government Code section 15619; California Labor Code section 1198.6; and Internal Revenue Code sections 6103, 7213, 7213A, and 7431.

I, _____ INITIALS acknowledge that unauthorized access, inspection, use, disclosure, or modification of confidential information , or any attempt to engage in such acts can result in:
- Administrative discipline, including but not limited to*: reprimand, suspension without pay, salary reduction, demotion, and/or dismissal from State service;*
- Criminal prosecution;
- Civil lawsuit; and
- Termination of contract.

I, _____ INITIALS expressly consent to the monitoring of my access to computer-based confidential information by the Franchise Tax Board, the Employment Development Department, the State Board of Equalization, and any other State agency designated by them.

CERTIFICATION

I certify that I understand information security is strictly enforced and wrongful access, inspection, use, modification, or disclosure of confidential information, or attempts to engage in such acts, is punishable as a crime and/or can result in disciplinary and/or civil action taken against me. I certify that I have received and read this confidentiality statement and have been provided the Information Security Requirement for Employees with Access to Confidential Information (FTB 7700) pamphlet.

Employee/Contractor Name (print) **Signature** **Date**

I certify that I reviewed and discussed this Confidentiality Statement with the employee named above.

Supervisor Name (print) **Signature** **Date**

This page left intentionally blank.

Notes:

1. True 2. True 3. True 4. False 5. False 6. True 7. False 8. False 9. False 10. True 11. False 12. True